STRATEGY RESEARCH PROJECT

CRITICAL INFRASTRUCTURE PROTECTION: A NEW DIMENSION OF U.S. NATIONAL SECURITY STRATEGY

BY

LIEUTENANT COLONEL DEBORAH J. BECKWORTH
United States Army

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

CRITICAL INFRASTRUCTURE PROTECTION: A NEW DIMENSION OF U.S. NATIONAL SECURITY STRATEGY

by

Deborah J. Beckworth
Lieutenant Colonel, U.S. Army

Colonel Danwill Lee
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Deborah Beckworth, Lieutenant Colonel, U.S. Army

TITLE: Critical Infrastructure Protection: A New Dimension of U.S. National Security Strategy

FORMAT: Strategy Research Project

DATE: 7 April 1999 PAGES: 42 CLASSIFICATION: Unclassified

One of the latest issues to hit the U.S. policy development scene in support of the U.S. national security core objective of enhancing U.S. security is critical infrastructure protection. Even though this complex and not well understood phenomenon has leaped to the forefront of U.S. national security strategy development in the latter part of the 1990's, it lies at the heart of national defense - transcending economic, diplomatic, military, and informational elements of power. Development and implementation of strong U.S. national security strategy is vital if this nation hopes to move in the right direction to identify vital, critical infrastructure vulnerabilities and make progress in eliminating or protecting those vulnerabilities. What is being done by the U.S. Government to get its arms around this issue? This paper examines national security strategy development, legislation, and resources being recommended, planned for, and applied to critical infrastructure protection.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I first want to recognize Colonel Danwill A. Lee, U.S. Army, Project Advisor for this research paper. I greatly appreciate his willingness to take on this task when I decided at mid-year to change my research topic. The latitude and flexibility he afforded me was invaluable to my ability to simultaneously complete this project, meet other academic requirements, and participate in class commitments. I could not have asked for more positive support and guidance.

Next, I want to acknowledge Lieutenant Colonel Robert Finn, who unknowingly provided outstanding support to my research efforts. By being a recipient of his regular terrorism updates via email, I was provided a myriad of current articles, official press releases, and sources covering U.S. domestic preparedness and critical infrastructure protection policy developments, that otherwise might have been overlooked.

Last, I want to thank my husband and children residing in Virginia, for their never-ending support of my academic requirements over the past year. As a geographical bachelor, their love and understanding enabled me to have a positive and personally rewarding experience at the U.S. Army War College.

CRITICAL INFRASTRUCTURE PROTECTION:
A NEW DIMENSION OF U.S. NATIONAL SECURITY STRATEGY

> We will launch a comprehensive plan to detect, deter, and defend against attacks on our critical infrastructures—our power systems, water supplies, police, fire, and medical services, air traffic control, financial services, telephone systems, and computer networks.
>
> —President William J. Clinton
> U.S. Naval Academy
> Commencement Address
> May 22, 1998

Topic du jour? Fad or fiction? Hoax or real need for concern? Are U.S. critical infrastructures vulnerable? One of the latest issues to hit the policy development scene in support of the U.S. national security core objective of enhancing U.S. security is critical infrastructure protection. Heavy dependence on computer systems ranging across every aspect of daily existence in this country, has created hundreds, maybe thousands of vulnerabilities only waiting to be exploited by belligerent parties seeking to do harm to the U.S. or its citizens. Even though this complex and not well understood phenomenon has leaped to the forefront of U.S. national security strategy development in the latter part of the 1990's, it lies at the heart of national defense - transcending economic, diplomatic, military, and informational elements of power.

There are those who profess that all this talk of critical infrastructure protection and associated threat capabilities such as cyberwarfare and weapons of mass destruction (WMD), are just the latest fad to generate a new "cottage industry" for the Washington beltway during an era of dwindling defense resources and no peer military threat. However, proponents for critical infrastructure protection counter the previous comment with the following question: Can this nation afford to ignore a potentially dangerous and devastating threat capability that if used, could severely impact, degrade, or even destroy critical infrastructures across the nation? While cyberwarfare systems and WMD capabilities are easy to define, solid identification, location, and intent of an actual threat—a belligerent party with a computer network attack or WMD capability and a hostile intent to do damage—is more difficult, if not impossible to predict.

Development and implementation of strong U.S. national security strategy is vital if this nation hopes to move in the right direction to identify vital, critical infrastructure vulnerabilities and make progress in eliminating or protecting those vulnerabilities. Ultimately, we must evolve to the point where we are confident that hostile attempts against our critical infrastructures will be met with no success or at best minimal degradation of operational capabilities.

U.S. security policy must range across many spectrums including proactive indications and warning (I&W) of pending attacks, engagement of active defense measures, sharing of information across government, military, law enforcement, and public sectors, as well as academia and private industry. If we are to gain the advantage against a rapidly expanding threat, we must move quickly, smartly, efficiently, and effectively. Only through thorough analysis and generous application of resources can the U.S. hope to tackle potential threats and genuinely protect this nation's critical infrastructures. Dialogue, coordination, and exchanges of ideas across sector domains is the only viable method to plan, develop, and coordinate successful responses against threats to U.S. critical infrastructures.

So are the U.S. government, public, and private sectors doing enough to protect critical infrastructures from harm? Has it fully grasped the daunting requirements of such a task? What is being done by the U.S. Government to get its arms around this issue? This paper attempts to answer these questions by examining current U.S. national security strategy development, policies, legislation, and resources being recommended, planned for, and applied to critical infrastructure protection.

EVOLUTION OF CRITICAL INFRASTRUCTURE PROTECTION

Critical infrastructures are systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of the nation. They include electrical power systems, telecommunications, gas and oil, banking and finance, transportation, water supply systems, government, and emergency services.[1] Even as late as 1997, there was no specific mention of critical infrastructure protection in U.S. national security strategy, beyond implied tasks imagined within the scope of physical security of our territory, safety of our citizens, and economic well-being. The idea of critical infrastructure protection as a national security interest is a current phenomenon, only rising to the surface in the last decade of the 20th Century. Not until the most recent publication of *the U.S. National Security Strategy (NSS), "A National Security Strategy for a New Century," October 1998,* do we see formal recognition of this issue as a national security concern.

Unfortunately, it has taken grave incidents to bring the idea of critical infrastructure protection to the concern of the U.S. Congress and the White House. Recent events within the U.S., such as the New York City World Trade Center (1993) and Oklahoma City Murrah Federal Building (1995) bombings brought realization to the fact that we no longer can claim sanctuary from domestic or international terrorism. The days of this

country being isolated from domestic or international threats are over. For example, from 1983 to 1991, the Federal Bureau of Investigation (FBI) identified 101 terrorist incidents in the U.S.[2]; the Department of Defense estimates that as many as 26 nations may possess chemical agents and/or weapons; the Central Intelligence Agency reports at least ten countries are believed to possess or conducting research on biological agents and weaponization; and at least 12 countries are developing formal information warfare programs.[3]

The roots of critical infrastructure protection policy grew from 1995, when President Clinton signed *Presidential Decision Directive 39 (PDD-39)*, which "directed the Attorney General to chair a Cabinet Committee to assess the vulnerability of the Nation's critical infrastructures and recommend measures to protect them."[4] Based on the guidance, the Attorney General set out to create the Critical Infrastructure Working Group (CIWG) comprised of representatives from a variety of agencies. This small group was one of the first in the U.S. to focus on not only threats to critical infrastructures, but also identification of actual vulnerabilities. In its January 1996 report to the President, the CIWG recommended further development of this issue. Their recommendations were twofold. One was to create a commission to assist and direct the development of U.S. national security strategy to protect

critical infrastructures. The second was an interim task force to evaluate, assess, and coordinate the U.S. Government's efforts and capabilities for response to infrastructure attacks.[5]

Based on the CIWG's recommendations and the growing concern over the impact and expansion of non-traditional threat capabilities including information warfare, weapons of mass destruction, and terrorism within the U.S., President Clinton signed *Executive Order 13010* on July 15, 1996, establishing the *President's Commission on Critical Infrastructure Protection (PCCIP)*. The PCCIP was chartered to conduct a comprehensive review and recommend a national policy for protecting critical infrastructures and assuring their continued operation. Justification for the PCCIP is found in a quote from the Commission's formal report:

> America's critical infrastructures underpin every aspect of our lives. They are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructures. We have to think differently about infrastructure protection today and for the future. The nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well being. In short, they are the lifelines on which we as a nation depend.[6]

In October 1997, the PCCIP issued its 100+ page report to the President with specific characterizations of five industry

sectors consisting of information and communications; banking and finance; energy - including electric power, oil, and gas; physical distribution; and vital human services. The characterizations include descriptions of sector vulnerabilities and associated recommendations to reduce or eliminate susceptibility to potential threats. Findings also included statements related to the lack of awareness of the extent of vulnerabilities in the services we all take for granted, the need for national focus on the topic, and the requirement for an advocate for infrastructure protection. While finding no evidence of an imminent threat to US critical infrastructures, the PCCIP stressed the widespread capability to exploit infrastructure vulnerabilities. The commission clearly articulated that the capability to do harm exists—particularly through information networks—and that the U.S. has little defense against it.[7]

As a result, on May 22, 1998, President Clinton, in his remarks to graduates of the U.S. Naval Academy, announced "a new program to sharply increase the tempo of federal efforts to protect the American people against terrorist attacks on their computer systems and physical facilities."[8] That same day, *Presidential Decision Directive 63 (PDD-63), The Critical Infrastructure Protection Directive*, was released. *PDD-63* is the culmination of an intense, interagency effort to evaluate

the recommendations provided by the PCCIP and produce a viable and innovative framework for critical infrastructure protection now and into the future. In *PDD-63*, President Clinton states:

> It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measure to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

Luckily, as a result of *PDD-63*, general critical infrastructure protection policy guidelines, organizations, recommended structures, and resources to begin addressing the problems and specific tasks to be accomplished under the auspices of a *National Infrastructure Assurance Plan* were created. *PDD-63* gave federal departments and agencies the guidance to take action.

This brief history shows that even though critical infrastructure protection was not mentioned in U.S. national security strategy until the latter part of 1998, there were other policies and actions underway, driving this concern to the forefront of national security consideration and debate. Since critical infrastructure protection policy is so new, it is impossible at this time to assess its clarity or consistency, except to say that hosts of government and non-government agencies, private and public organizations and businesses, as well as academia, are intently listening, closely watching, and

looking for innovative ways to manage this issue. It is beginning to make its way out of the Executive Branch and into the Legislative Branch through Congressional Hearings such as one held on June 11, 1998, by the U.S. House of Representatives Committee on National Security, where the U.S. Administration's program for critical infrastructure protection was reviewed. As legal debates unfold, the Judicial Branch surely will be involved as well.

CRITICAL INFRASTRUCTURE PROTECTION POLICY REVIEW

Current critical infrastructure protection policy now is found in five crucial documents: *U.S. National Security Strategy (U.S. NSS), October 1998; Presidential Decision Directive 63 (PDD-63), May 1998; Presidential Decision Directive 62 (PDD-62), 1998; U.S. Executive Order 13010 (EO 13010)(as amended March 1998);* and the *Nunn-Lugar-Domenici (NLD) Act of 1996.* These strategies, directives, and legislation formulate U.S. policy for the scope, depth, and direction of critical infrastructure protection across government, public and private domains and range in context from strategic, general guidance to more specific objectives, milestones, capabilities, and actions.

As stated earlier, ***US National Security Strategy, "A National Security Strategy for a New Century," October 1998,*** is the first U.S. NSS specifically to mention critical infrastructure protection. Only after pressure from the other policies mentioned above and the publication of PCCIP's *"The Report of the President's Commission on Critical Infrastructure Protection: Critical Foundations, Protecting America's Infrastructures,"* in October 1997, did the White House finally include this security concern within the framework of the *NSS.*

The current *NSS* succinctly addresses the changing nature of today's global threats and defines the nation's three core security objectives as enhancing security, bolstering America's

economic prosperity, and promoting democracy abroad. In the preface signed by President Clinton, he states,

> Protecting our citizens and critical infrastructures at home is an essential element of our [security] strategy. Potential adversaries...will be tempted to disrupt our critical infrastructures, impede government operations, use weapons of mass destruction against civilians, and prey on our citizens overseas. These challenges demand close cooperation across all levels of government—federal, state and local—and across a wide range of agencies...Protecting our critical infrastructure requires new partnerships between government and industry...if we are to ensure our safety at home and avoid vulnerabilities...and to protect our interests abroad.

More specifically, critical infrastructure protection is addressed in the *NSS* as a subcategory of the core objective of "enhancing security at home and abroad." While brief and only three paragraphs in length, four critical points are outlined and serve as drivers to all subsequent critical infrastructure protection policies. First is a general U.S. security statement acknowledging the reliance and interdependence of the government, military, and economic sectors on physical and information systems. Second is a challenge for government and private sectors to cooperatively work to ensure availability and reliability of services. Third is an articulation of an ultimate operational standard by which any attack or degradation of a critical infrastructure function must be brief, infrequent, manageable, isolated, and minimally detrimental to the welfare of the United States.[9] Fourth is the formal mission statement of

the National Infrastructure Protection Center (NIPC), a subordinate organization of the Federal Bureau of Investigation (FBI), as an integrator and focal point for federal, state, and local governments, as well as the private sector on information pertaining to critical infrastructure threats. In summary, the *NSS* sets the tone for all subsequent and future critical infrastructure protection policy, programming, and resourcing actions well into the 21st Century.

Presidential Decision Directive 63 (PDD-63), The Critical Infrastructure Protection Directive, published 22 May, 1998, is the policy that transitioned the short-term policy found in *Executive Order 13010* to a broad, long-term approach needed for inclusion of critical infrastructure protection as a national security strategy issue as we move into the 21st Century. It specifically identifies critical infrastructure protection as a national security priority. *PDD-63's* "intent is to put in place a process that will take the necessary measures to eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber-based systems."[10] It "calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. It requires immediate federal government action including risk assessment and planning to reduce exposure to attack. It stresses the critical

importance of cooperation between the government and the private sector by linking designated agencies with private sector representatives."[11]

Five strategic objectives (ends) encompass *PDD-63*. They include:

- building a public-private partnership;
- conducting education and awareness across industry, government, and the general public;
- promotion of "best practices";
- examining legislative and legal issues surrounding executive branch legislative authorities and budgetary priorities; and,
- enhancing research and development efforts and coordination of the government, private, and public sectors to encourage efficient use innovative technologies and methodologies.

The *PDD* also calls for specific ways to meet these objectives to include:

- identifying the issue as a national security priority;
- establishing a national commitment of protection within five years and an interim security capability by the year 2000;
- developing a new mechanism to coordinate critical infrastructure protection planning within the government;
- establishing other mechanisms to encourage the private sector to create its own mechanism for information sharing and cooperation;
- developing sector plans for each sector of our critical infrastructure;

- developing a national plan drawing on the sector plans; challenging the Federal Government to lead by example in securing its own systems;

- establishing a public-private partnership to accomplish its goals; and,

- appointing functional coordinators to address crosscutting issues.[12]

Presidential Decision Directive 62 (PDD-62), Combating Terrorism, was released in early 1998, and reaffirms government agencies' counter-terrorism roles and strengthens the Interagency coordination process through the creation of the Office of the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism. It also emphasizes the role of consequence management, especially regarding the threat of chemical or biological WMD.

Executive Order 13010 (EO 13010) (as amended March 10, 1998), actually published before the 1998 *NSS*, articulates the need for the government and private sector to work together to develop a strategy for protecting critical infrastructures and assuring their continued operation. It was the first attempt to bring critical infrastructure protection on the national security interest radarscope. It establishes short-term, definable, and achievable objectives (ends) while dictating the specific methods (ways) and resources (means) to be applied to encourage our understanding of this problem. It codifies the belief that certain national infrastructures "are so vital that their

incapacity or destruction would have a debilitating impact on the defense or economic security of the U.S."[13] It established the PCCIP, a myriad of oversight and approval committees, and assigned membership to include the Departments of Treasury, Justice, Defense, Commerce, Transportation, Energy, and the Central Intelligence Agency (CIA), Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA). Of key importance, it detailed the mission of the PCCIP to identify and consult with public and private infrastructure sectors, assess the scope of vulnerabilities and threats to critical infrastructures, determine legal policies raised by efforts to protect critical infrastructures, recommend comprehensive national policy and implementation strategy, propose statutory or regulatory changes necessary to implement recommendations, and produce reports as required. It also established the Infrastructure Protection Task Force (IPTF) to provide, facilitate, and coordinate, the provision of and expert guidance to critical infrastructures in an attempt to detect, prevent, halt, or confine an attack.

The ***Nunn-Lugar-Domenici (NLD) Act of 1996***, actually was an earlier attempt to highlight the issue of WMD response and as such, has a relation to critical infrastructure protection. It focused attention on the growing need for U.S. capabilities to mitigate the consequences of domestic and foreign WMD attacks in

both domestic preparedness and force protection roles. The *NLD Act of 1996*, was enacted as *Title XIV of the FY97 Defense Authorization Act* that same year. "Seeking to enhance domestic preparedness and response capabilities, this legislation provided more funding to improve the capabilities of federal, state, and local emergency response agencies to prevent and, if necessary, respond to domestic terrorist incidents involving WMD."[14] Of note, it was the *NLD*, which first proposed a training program calling for a goal of training responders in 120 cities across the U.S. Additionally, as a result of the *NLD*, the U.S. National Guard has established ten Rapid Assessment and Initial Detection (RAID) Teams, as part of DOD's overall efforts to support local, state, and federal civil authorities in the event of an incident involving WMD within the U.S. Each has an assigned geographic region and is charged with reaching the scene of a WMD attack within four hours to assist local civilian responders.

RESOURCING OF CRITICAL INFRASTRUCTURE PROTECTION

Resourcing of the stated or implied requirement in the above policy documents reviewed above total in the billions. In a 22 January, 1999, White House Press Release, it was reported that the *President's Fiscal Year (FY) 2000 Budget* included requests of $1.385 billion for domestic preparedness against WMD and $1.464 billion for critical infrastructure and computer protection. In addition, it called for $7.162 billion for conventional counter-terrorism security programs. Buried within these budget lines are hosts of requests ranging from federal, state, and local government programs to medical research and response training. These requests call for investment in new programs to combat unconventional threats, significant increases in research and development of new vaccines and other therapeutics, a network of labs to conduct analysis of biological agents, improvements in public health surveillance systems, fire fighter training, and first responder training across the nation.

Highlights of critical infrastructure protection initiatives outlined in the *President's FY 2000 Budget* include:

- Biological/Chemical - an increase of $30 million above previous levels for research of new vaccines and medications and $52 million to increase national stockpiles of vaccines and medications;

- Nuclear - $381 million for research and development of treatments against nuclear contamination and disposition of nuclear material;

- Cyberwarfare - $500 million for a Critical Infrastructure Applied Research Initiative, $2 million in addition to DOD funding to design and evaluate other Federal agency information systems, $3 million to create new scholarship programs to retrain, retain, and recruit computer science students to bring expertise to the U.S. Government;

- Detection/Response - an additional $15 million to fund public detection programs, an additional $13 million to support creation of new metropolitan medical response teams, and $611 million for training and equipping emergency personnel across the nation to respond to WMD contingencies; and,

- Prevention/Security - $206 million to support protection of U.S. Government facilities and $8.547 billion for all anti-terrorism and counter-terrorism programs including additional security measures at diplomatic and consular facilities.[15]

In addition to these robust fiduciary requests, hosts of actions already have been underway for some time. Over the past year, the Department of Defense (DOD) trained over 15,000 first responders and fire fighting personnel in 52 cities to respond to terrorist use of biological or chemical weapons. Furthermore, it is expected that by the end of fiscal year 1999, DOD will train response personnel in at least 16 more cities.[16]

While federal agencies have been tasked and a myriad of new critical infrastructure protection committees, task forces, and working groups formed, the actual personnel and budget resources necessary to implement a viable critical infrastructure program to meet the President's *NSS* '98 goal are just beginning to be

realized. It will be several years before we can assess if the requests in the *President's FY 2000 Budget* and future budgets are suitable and sustainable at the federal level. Frankly, ground truth only will be realized after some old fashioned trial and error along with more in-depth analysis and determination of susceptibilities within our critical infrastructures.

The U.S. then must weigh these susceptibilities against future threat projections and conduct aggressive and continual risk assessment to determine actual critical vulnerabilities—better called 'points of catastrophic failure'—against ever evolving threat capabilities and intentions. Only then can the U.S. Government conduct an accurate cost benefit analysis and determine appropriate resourcing levels. Most certainly, this task will not be easy, nor will anyone or any agency ever find a single solution to fix the problem. Critical infrastructure protection is too complex to fix quickly and easily; it crosses over too many domains and too many people to be simple.

With time and focused attention, the U.S. can come to workable and viable solutions for implementation across government, public, and private sectors. The only risks are that: (1) the U.S. Government remains overconfident, does nothing, and suffers what may, or (2) overreacts, over estimates the threat, and pours a lot of wasted man-hours and dollars at a problem while

never reaching solutions. Even so, neither risk outweighs the potential damage that attacks to U.S. critical infrastructures could cause to our citizens and the security framework of the nation. "The key to success will be in balancing the ends, ways, and means associated with this problem. The Information Age will unfold through time, consolidating and defining itself as it evolves. The same is true for Information Age warfare, which no one can suddenly invent, but which rather must develop organically at its own pace over the coming decades, taking turns and assuming forms that are indiscernible to us today. Our best posture is vigilant observation, active trial-and-error, and continued adaptation, keeping our eye always on the longer-range picture."[17]

FUTURE THREAT PROJECTION

One of the nation's toughest strategic challenges will be the identification of the threat and proactive indications and warning (I&W) of impending threat attacks against critical infrastructures. To enable more proactive threat identification, I&W of threat attacks to critical infrastructures, and consequence management response actions, the U.S. Government must assess how to best use all resources at hand to balance its prevention (proactive), protection (defensive), and response (offensive) strategies.

Future terrorists will benefit from technology and shift their tactics to asymmetrically move and operate within a new international jungle using a range of weapons which could include the simplest of rifles, pistols, and bombs, to more sophisticated biological and chemical agents, nuclear devices, and information warfare technology. "The new threat environment may see the emergence of a wide variety of sub-national and transnational groups intent on venting their frustrations with Washington for what they perceive to be a lack of support for their causes or, conversely, for supporting their adversaries."[18]

Rogue states and non-state sponsored organizations such as separatists, militant fundamentalists, drug cartels, and criminals will continue to exist and pose an immediate challenge to critical infrastructure security of the U.S.[19] The FBI

reports an increase in the number of credible domestic threats involving WMD from a number of 68 active cases in 1997, to 86 investigations in the first nine months of 1998. They speculate that the danger imposed by terrorism and the potential use of WMD will continue well into the foreseeable future. Covert, clandestine, or state-sponsored groups could use viruses such as anthrax and smallpox against critical infrastructures. Of critical concern to national leaders is the trend suggesting the real possibility of a biological terrorist event in the U.S. Open source reports of "uprooted weapon scientists from Iraq, Russia, and South Africa, hunting for new jobs and spreading biological warfare secrets; terrorists, including Osama bin Laden, showing increasing interest in biological agents; and, radical states with reputations for supporting terror, such as Iran and Libya, seeking biological weapons,"[20] are on the rise.

The threat posed by "the electronic web of computers and information technology (IT) virtually touches every element of the U.S. domestic infrastructure."[21] "Potential enemies 'information abilities' points to a new form of warfare that could threaten the U.S. The threat of cyberwarfare is real. Our potential enemies tend to be multispectral. They are either unpredictable or they are unknown."[22] All indications are that reliance on IT will last well beyond 2010. For this reason, the U.S. must continue to address the issue of critical

infrastructure protection as a national security issue well into the future. Various studies highlight the fact that "modern nations are extraordinarily complex systems of networks that depend on the synergistic interplay of their various components to function effectively. For example, the increasing dependence on supervisory control and data acquisition (SCADA) systems linked by digitized and computerized information transmissions"[23] within our critical infrastructure systems will continue to produce strategic security vulnerabilities for the U.S. The impact of potential cyberwarfare on U.S. diplomacy, economic stability, military capabilities, and information assurance is beginning to be realized. Through strategic level exercises and studies, the impact of terrorist or even state-sponsored attacks on U.S. critical infrastructures is making its way into planning and programming of projected offensive and defensive capabilities.

With this type of threat and new capabilities on the forefront, it will be a challenge for both U.S. domestic and international law enforcement and intelligence agencies to cope with the growing problem—let alone get ahead of it. The future threat environment is projected to critically impact the entire U.S. intelligence system—strategic through tactical—and, that future threat is just around the corner. The application of limited intelligence resources ranging from technical

intelligence, to human and open source intelligence must be assessed against intelligence production requirements generated by intelligence consumers. Intelligence consumers must think in new ways and assess the types of missions they will be expected to execute in the future. They must consider the types of threat and the threat capabilities they might encounter. Only after this in-depth analysis can they determine if standing intelligence requirements meet their needs. If not, then consumers must create new intelligence requirements for validation and satisfaction.

CONCLUSION

It really is too early to judge the success or failure of courses of actions in the critical infrastructure arena, but as this paper suggests, actions are underway across the nation to examine and tackle this issue in a proactive manner. The U.S. Government, through organizations such as DOD, Justice, and the NIPC within FBI, aggressively must seek out, inform, educate, and aid the public and private sectors in order to make critical infrastructure protection a reality.

Unfortunately, there are critics of ongoing efforts. Some think that while successful in beltway terms, the PCCIP report did not provide a credible and comprehensive threat and vulnerability assessment, a list of specific problems, statistics, and detailed case studies, or a coherent plan for constructive change. Other experts, such as William Church, managing director of the San Francisco-based Centre for Infrastructural Warfare Studies (CIWARS), disagree with the concept that terrorists have the capability to coordinate attacks on the U.S. computer infrastructure. Mr. Church states, "As of right now, there is no terrorist organization that we know of with the necessary skills. Cyber attacks on a national power grid or communications infrastructure can be crippling in theory, but the weapons have yet to be proven."[24] The bottom line—"we still don't know how vulnerable we are, and we have no

idea how to go about the long-term process…."[25] To many, identification of vulnerabilities will determine success or failure of this program.

Even though skeptics are out there, recommend that government, public, and private sectors continue to follow the guidance set forth in *PDD-63*. It is a roadmap to the future that can be modified as more is known and relationships are established. Furthermore, it is a positive sign that the Executive, Legislative, and Judicial Branches, as well as the DOD, FBI, CIA, NSA, and FEMA, are taking a great interest in this new national security interest looming on the horizon.

Additionally recommend that a small task force be created by DOD to assess how Defense assets, to include Active and Reserve forces can best be used in support of the public and private domains, within the limitations stated in the *posse comitatus* law. DOD has excellent communications, intelligence, counterintelligence, transportation, medical, and decontamination resources. These resources are spread across the country in support of U.S. military forces and installations. It may be feasible for these resources to partner with local, state, and federal agencies for anything from I&W, vulnerability assessments, information assurance, consequence management, medical response, and decontamination in support of critical infrastructure attacks. But, we will not

know the possibilities unless a thorough examination of all barriers, to include legal, is made. We must think through all possible and viable options if we are to protect our critical vulnerabilities in a smart, efficient, and effective manner.

Cities across the nation are beginning to develop an awareness and concern over the possibility of terrorist actions. From Baltimore, Maryland, to Monterey, California, cities are conducting exercises to better train emergency reaction, medical, law enforcement, fire, search and rescue, and consequence management personnel to better handle a WMD or WMD-like catastrophe. While some may view this as an over-reaction by paranoid governments and policy makers and poor resource management over media hype about terrorism, the U.S. cannot afford to ignore homeland defense or turn its back to a quickly expanding and more elusive threat.

WORD COUNT = 5,811

ENDNOTES

[1] "Fact Sheet: President's Commission on Critical Infrastructure Protection," available from <http://www.pccip.gov/backgrd.html>. Internet; accessed 30 September 1998, 1.

[2] "Federal Emergency Management Agency Backgrounder - Terrorism Facts," available from <http://www.fema.gov/library/terror.html>. Internet; accessed 31 January 1999, 1-2.

[3] Donald Harrington <donald.harrington@SBCCOM.APGEA.ARMY.MIL>, "INFO WAR: CIA's View," electronic mail message to Deborah Beckworth <beckworthd@awc.carlisle.army.mil>, 25 March 1999.

[4] Michael Vatis, Deputy Assistant Director Nation Infrastructure Protection Center, "Testimony to the Senate Judiciary Subcommittee on Terrorism, Technology and Government Information," 10 June 1998, available from <http://www.usia.gov/current/news/topic/global/98061101.pgi.html?/products/washfile/newsitem/shtml>. Internet; accessed 31 January 1999, 1.

[5] Ibid., 2.

[6] "Critical Foundations, Protecting America's Infrastructures," The Report of the President's Commission on Critical Infrastructure Protection, October 1997, available from <http://www.pccip.gov>. Internet; accessed 30 September 1998, vii.

[7] Robert T. Marsh, Chairman PCCIP, "President's Commission on Critical Infrastructure Protection," letter for The President, Washington, D.C., 13 October 1997.

[8] Paul Rodgers, "CIAO/PDD-63 Implementation," 27 August 1998, available from <http://www.ciao.gov/sbrodgers27081998.html>. Internet; accessed 31 January 1999, 1.

[9] National Security Strategy of the United States, A National Security Strategy for a New Century, The White House, October 1998, 21.

[10] Dr. Jeffrey A. Hunker, Director, Critical Infrastructure Assurance Office, "Statement Before the House National Security Committee, Military Procurement Subcommittee, and Military Research and Development Subcommittee," June 11, 1998, available from <http://www.ciao.gov/sbhunker11june1998.html>. Internet; accessed 30 September 1998, 8.

[11] "Summary of Presidential Decision Directives 62 and 63," available from <http://www.ciao.gov/6263summary.html>. Internet; accessed 30 September 1998, 3.

[12] Dr. Jeffrey A. Hunker, 8-9.

[13] Executive Order 13010 (as amended), dated July 15, 1996, available from <http://www.pccip.gov/eo13010.html>. Internet; accessed 30 September 1998, 1.

[14] Hicks & Associates, Inc., "Homeland Defense: Threats and Policies in Transition," available from <http://www.terrorism.com/homeland/CT&CIAfinal.html>. Internet; accessed 31 January 1999, 3-4.

[15] The White House, Office of the Press Secretary, "Fact Sheet: Funding for Domestic Preparedness and Critical Infrastructure Protection," 22 January 1999, 1-2.

[16] The White House, Office of the Press Secretary, "President Clinton Unveils New Efforts to Combat Terrorism in an Address to the International Association of Firefighters," 15 March 1999, 1.

[17] Major General Robert H. Scales, Jr., "Part IV: Roundtable on Future Responses," in Challenging the Unites States Symmetrically and Asymmetrically: Can America Be Defeated?, ed. Colonel Lloyd J. Matthews (Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 1998), 330-333.

[18] Stephen Sloan, "Terrorism: How Vulnerable is the United States?" available from <http://www.terrorism.com/terrorism/sloan.html>. Internet; accessed 30 September 1998.

[19] Hans Binnendijk, 1998 Strategic Assessment, Engaging Power for Peace (Washington, D.C.: U.S. Government Printing Office, 1998), 7.

[20] Steve Macko, "The Threat of Biological Attack -- Is America Prepared?" <rzielinski@nhpsm.ang.af.mil> article forwarded via electronic mail message to Deborah Beckworth <beckworthd@carlisle.awc.army.mil>, 20 January 1999.

[21] Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, eds., "Information Assurance: Implications to National Security and Emergency Preparedness by James Kerr," in Cyber War: Security, Strategy, and Conflict in the Information Age (Fairfax, Virginia: AFCEA International Press, 1996), 263.

[22] C.L. Staten <sysop@emergency.com>, "Publication 3-13, Joint Doctrine for Information Operations," electronic mail message to Deborah Beckworth <beckworthd@awc.carlisle.army.mil>, 10 March 1999.

[23] Campen, Dearth, and Gooden, eds., "Strategic Information Warfare and Comprehensive Situational Awareness," 189.

[24] C.L. Staten, "Pentagon Computers Under Attack?" EmergencyNet News Special Report, 8 March 1999, 1-3.

[25] Matthews, ed., "Takedown: Targets, Tools, and Technocracy by Robert D. Steele," 119-120.

BIBLIOGRAPHY

"Federal Emergency Management Agency Backgrounder - Terrorism Facts." Available from <http://www.fema.gov/library.terror.html>. Internet. Accessed 31 January 1999.

Binnendijk, Hans. 1998 Strategic Assessment, Engaging Power for Peace. Washington, D.C.: U.S. Government Printing Office, 1998.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Gooden, eds. Cyber War: Security, Strategy, and Conflict in the Information Age. Fairfax, VA: AFCEA International Press, 1996.

"Critical Foundations, Protecting America's Infrastructures." The Report of the President's Commission on Critical Infrastructure Protection. October 1997. Available from <http://www.pccip.gov>. Internet. Accessed 30 September 1998.

Executive Order 13010 (as amended), July 15, 1996. Available from <http://www.pccip.gov/eo13010.html>. Internet. Accessed 30 September 1998.

"Fact Sheet: President's Commission on Critical Infrastructure Protection." Available from <http://www.pccip.gov/backgrd.html>. Internet. Accessed 30 September 1998.

Harrington, Donald <donald.harrington@SBCCOM.APGEA.ARMY.MIL>. "INFO WAR: CIA's View." Electronic mail message to Deborah Beckworth <beckworthd@awc.carlisle.army.mil>. 25 March 1999.

Hicks & Associates, Inc. "Homeland Defense: Threats and Policies in Transition." Available from <http://www.terrorism.com/homeland/CT&CIAfinal.html>. Internet. Accessed 31 January 1999.

Hunker, Jeffrey A., Dr., Director, Critical Infrastructure Assurance Office. "Statement Before the House National Security Committee, Military Procurement Subcommittee, and Military Research and Development Subcommittee." 11 June 1998. Available from <http://www.ciao.gov/sbhunker11june1998.html>. Internet. Accessed 30 September 1998.

Macko, Steve. "The Threat of Biological Attack -- Is America Prepared?" Electronic mail message from <rzielinski@nhpsm.ang.af.mil> to Deborah Beckworth <beckworthd@carlisle.awc.army.mil>. 20 January 1999.

Marsh, Robert T., Chairman PCCIP. "President's Commission on Critical Infrastructure Protection," Letter for The President. Washington, D.C., 13 October 1997.

Scales, Robert H., Jr., Major General. "Part IV: Roundtable on Future Responses." Challenging the Unites States Symmetrically and Asymmetrically: Can America Be Defeated?, ed. Colonel Lloyd J. Matthews, 330-333. Carlisle Barracks, PA: U.S. Army War College Strategic Studies Institute, 1998.

National Security Strategy of the United States. A National Security Strategy for a New Century. Washington, D.C.: The White House. October 1998.

Rodgers, Paul. "CIAO/PDD-63 Implementation." 27 August 1998. Available from <http://www.ciao.gov/sbrodgers27081998.html>. Internet. Accessed 31 January 1999.

Sloan, Stephen. "Terrorism: How Vulnerable is the United States?" Available from <http://www.terrorism.com/terrorism/sloan.html>. Internet. Accessed 30 September 1998.

Staten, C.L. "Pentagon Computers Under Attack?" EmergencyNet News Special Report. 8 March 1999.

Staten, C.L. <sysop@emergency.com>. "Publication 3-13, Joint Doctrine for Information Operations." Electronic mail message to Deborah Beckworth <beckworthd@awc.carlisle.army.mil>. 10 March 1999.

"Summary of Presidential Decision Directives 62 and 63." Available from <http://www.ciao.gov/6263summary.html>. Internet. Accessed 30 September 1998.

The White House. Office of the Press Secretary. "Fact Sheet: Funding for Domestic Preparedness and Critical Infrastructure Protection," 22 January 1999.

The White House. Office of the Press Secretary. "President Clinton Unveils New Efforts to Combat Terrorism in an Address to the International Association of Firefighters," 15 March 1999.

Vatis, Michael, Deputy Assistant Director Nation Infrastructure Protection Center. "Testimony to the Senate Judiciary Subcommittee on Terrorism, Technology and Government Information." 10 June 1998. Available from <http://www.usia.gov/current/news/topic/global/98061101.pgi.html?/products/washfile/newsitem/shtml>. Internet. Accessed 31 January 1999.